# NATIONAL INFRASTRUCTURE PROTECTION CENTER

# HIGHLIGHTS

*A publication providing information on infrastructure protection issues, with emphasis on computer and network security matters.*


**Issue 10-01**
**November 10, 2001**

*Editors*: Linda Garrison
Martin Grand

---

- **Extremist Groups: New Organizational Models Empowered by Networked Information Systems**
- **Information Sharing and Analysis Center-Water Supply Sector**
- **Connect it and They Will Come: No Grace Period for Internet-connected Hosts**

---

For more information, or to be added to the distribution list, please contact the NIPC Watch at nipc.watch@fbi.gov or (202)323-3204.

We welcome your comments and suggestions for improving this product. To provide comments, contact the Editors at (202) 324-0334 or (202) 324-0353.

**Extremist Groups: New Organizational Models**
**Empowered by Networked Information Systems**

Because authorities are often able to prevent violent extremist plots by learning of impending attacks, some extremist groups have adopted new organizational models in order to mitigate damage to their operations.

One organizational model that has attracted attention over the past decade is the development of "leaderless resistance" resulting in decentralized organizational structures. In contrast to a traditional hierarchical command structure, leaderless resistance bases itself on cells comprised of a few members or even a single individual who operate without identifiable central direction. An individual cell's members have limited or no knowledge at all of the identity of members of other cells, so as to limit damage from penetration by authorities. Groups across the ideological spectrum have adopted aspects of the leaderless resistance.

Extremist groups are increasingly adopting the power of modern communications technology. An extremist organization whose members get guidance from e-mails or by visiting a secure web site can operate in a coordinated fashion without its members ever having to meet face to face with other members of the organization. There are several aspects of leaderless resistance which are particularly facilitated by modern information technology:

**Recruiting and Propaganda**. In the absence of a coordination and training authority, new members must be indoctrinated into the fold and steeped in the movement's beliefs by a steady stream of propaganda. The Internet is an ideal conduit for this information flow.

**Secure Communications**. Readily accessible online communication in many countries, such as free email accounts, Internet Relay Chat, and Web-based bulletin boards, make it difficult to link a message with a particular individual. More sophisticated technology, such as anonymous remailers, encryption, or steganography, can make identification and attribution extremely difficult.

**Coordination and Consensus**. Through Internet gathering points, such as Internet relay chat (IRC) or ICQ (I seek-you) widely dispersed members can share ideological and operational information, enabling them to centralize their shared world view into independently actuated agendas in support of a common (and sometimes violent) goal.

**To date, cyber attacks by extremists have largely been limited to relatively unsophisticated efforts such as the email bombing of ideological foes or the publication of threatening content. However, increasing technical competency in these groups is resulting in an emerging capability for network-based attacks, including those targeting our nation's infrastructures. Extremist groups have proven themselves capable of carrying out acts of violence, and the leaderless resistance strategy makes it even more difficult for authorities to foresee actions by such groups.**

**Information Sharing and Analysis Center – Water Supply Sector**

This article continues the series of overviews of critical infrastructure industry initiatives established in response to Presidential Decision Directive 63 (PDD-63).

**PDA-63 and the Water Supply Sector**

Since the beginning of the government's formal critical infrastructure protection (C.P.) initiatives in the mid-1990s, our leaders have realized the importance of safeguarding the nation's water supply and water distribution infrastructure. In keeping with this priority, PDA-63 designated the Environmental Protection Agency (EPA) as the government's lead agency to spearhead efforts in this sector. The EPA subsequently named Diane VanDe Hei, executive director of the Association of Metropolitan of Water Agencies (AMWA), as Water Sector Liaison. The AMWA is an industry group representing some of the country's largest municipal water utilities.

**The Water Sector Critical Infrastructure Protection Advisory Group**

In July 2000, NIPC representatives contacted Ms. VanDe Hei regarding establishing an information sharing and analysis center (ISAC) for the water sector. It was decided that AMWA must reach out to all the national water associations and form a sector-wide advisory group.

Consequently, the Water Sector Critical Infrastructure Protection Advisory Group was established in December 2000. It consists of thirteen water industry members from the various national water associations in addition to government representatives from the EPA, the Department of Energy, and the NIPC. This group is in the process of developing a Water Sector CIP Plan that will include the establishment of the ISAC for the sector.

**Water Sector ISAC Status**

The EPA has provided start-up money to the AMWA to establish the Water Sector ISAC. In the interim, the NIPC is treating the AMWA itself as an operational Water Sector ISAC. NIPC sends out its alerts and advisories as well as CyberNotes and analytical publications to AMWA. The AMWA then disseminates these products to other national water associations, who in turn distribute them to their membership.

In the wake of the September 11 terrorist attacks, the NIPC provided threat update briefings to the AMWA as well as to the CIP Advisory Group. With the encouragement from the Advisory Group, the AMWA accelerated and achieved its timetable for ISAC operational status ahead of schedule. The AMWA has recently provided a detailee to the NIPC on a part-time basis.

**Further information on the status of the Water Sector ISAC is available by contacting either AMWA's Susan Tramposch by telephone at 202-331-2820 or the NIPC's representative, SSA Anita Dickens, at 202-324-0362. Further information on the ISAC is also available on the AMWA's web site at http://www.amwa.net/isac/index.html.**

**Connect It and They Will Come: No Grace Period for Internet-connected Hosts**

New Internet victim or host computers can be located by malicious parties in a short period of time. Computer systems which are not properly secured may be compromised within days or even minutes of connecting to the Internet due to the increased usage of automated scanning tools.

The hypothesis that newly connected Internet hosts can be quickly found by hackers has been confirmed by researchers from the Honeynet Project, a computer security research group. In a study published earlier this year, the group reported the following observations:

- One of the project's research computer systems was compromised a mere 15 minutes after being connected to the Internet.
- Seven computers running default installations of a popular Linux distribution were attacked within three days of connecting to the Internet.
- A default Windows 98 system was compromised five times in less than four days.

These and other observations belie the common misconceptions many users and some system administrators have about connecting to the Internet:

- Misconception 1: "I won't tell anyone about my computer, so no one will ever even find it."
- Misconception 2: "There are millions of computers connected to the Internet, so the odds against anyone targeting my computer are very low."
- Misconception 3: "With all the other important and high-profile servers out there on the Internet, no one would want to break into my computer."

The impact of automated scanning tools allows individuals to scan tens of thousands of Internet addresses in a short time. Like many home systems, the computers used in the Honeynet Project were not advertised or associated with a particular company. No one had any way of knowing the systems were connected to the Internet except by discovering them through scanning ranges of Internet addresses, looking for vulnerable hosts to exploit. After compromising the targets, intruders can examine the victimized computer for exploitable information such as personal information that can be used for identity theft, or they can utilize the host to attack other systems on the Internet.

Many users hook up to the Internet with the intent of implementing security measures in the future. It is imperative that users plan on security **before** they connect their computers to a public network. Some good starting points for identifying potential problem areas are the following online resources:

- The NIPC's "Seven Simple Computer Security Tips for Small Business and Home Computer Users" at **http://www.nipc.gov/warnings/computertips.htm**
- The SANS/FBI list of the Twenty Most Critical Internet Security Vulnerabilities at **http://66.129.1.101/top20.htm**
- NIPC's *CyberNotes* at **http://www.nipc.gov**
- **The Honeynet Project --** http://project.honeynet.org